

Bitdefender® Mobile Security



USER'S GUIDE



Bitdefender Mobile Security User's Guide

Publication date 05/25/2018

Copyright© 2018 Bitdefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.



Table of Contents

1. Protection Features	1
2. Getting Started	2
3. Malware Scanner	7
4. Account Privacy	10
5. Web Protection	12
6. VPN	14
7. Anti-Theft Features	17
8. App Lock	22
9. Reports	27
10. WearON	28
11. Settings	29
12. About	30
13. Bitdefender Central	31
14. Frequently Asked Questions	35
15. Getting Help	41



1. PROTECTION FEATURES

Bitdefender Mobile Security protects your Android device with the following features:

- Malware Scanner
- Account Privacy
- Web Protection
- VPN
- Anti-Theft, including:
 - Remote location
 - Remote device lock
 - Remote device wipe
 - Remote device alerts
- App Lock
- Reports
- WearON

You can use the product features for 14 days, free of charge. After the period expires, you need to purchase the full version to protect your mobile device.



2. GETTING STARTED


Device Requirements

Bitdefender Mobile Security works on any device running Android 4.0.3 and up. An active internet connection is required for in-the-cloud threat scanning.


Installing Bitdefender Mobile Security

● From Bitdefender Central

● On Android

1. Go to: <https://central.bitdefender.com>.
2. Sign in to your Bitdefender account.
3. Tap the  icon in the upper-left corner of the screen, then select **My Devices**.
4. Tap **INSTALL LOCAL PROTECTION**.
5. Select **Bitdefender Mobile Security** from the list, then tap **GO TO GOOGLE PLAY**.
6. Tap **INSTALL** in the Google Play screen.

● On Windows, macOS, iOS

1. Go to: <https://central.bitdefender.com>.
2. Sign in to your Bitdefender account.
3. Press the  icon in the upper-left corner of the screen, and then **My Devices**.
4. Press **INSTALL LOCAL PROTECTION**.
5. On Windows and macOS, click the **On another device** link.
On iOS, tap **Want to protect other devices?**
6. Choose **Android**.
7. Select **Bitdefender Mobile Security** from the list, then press **CONTINUE**.
8. Type an email address in the corresponding field, then press **SEND**.



9. Access your email account from your Android device, then tap the **GET IT ON Google Play** button.

You are redirected to the **Google Play** app.

- 10 Tap **INSTALL** in the Google Play screen.

● From Google Play

Search for Bitdefender Mobile Security to locate and install the app.

Alternatively, scan the QR Code:



QR Code

To finish the installation process, you have to agree with the Subscription Agreement. Please take some time to read the Subscription Agreement as it contains the terms and conditions under which you may use Bitdefender Mobile Security.

Tap **CONTINUE** to proceed to the next window.

Sign in to your Bitdefender account

To use Bitdefender Mobile Security, you must link your device to a Bitdefender, Facebook, Google, or Microsoft account by signing in to the account from the app. The first time you open the app, you will be prompted to sign in to an account.

If you installed Bitdefender Mobile Security from your Bitdefender account, the app will attempt to automatically log in to that account.

To link your device to a Bitdefender account:

1. Open Bitdefender Mobile Security.



2. Type your Bitdefender account email address and password in the corresponding fields. If you do not have a Bitdefender account and want to create one, select the corresponding link.

3. Tap **SIGN IN**.

To log in using a Facebook, Google, or Microsoft account, tap the service you want to use from the **OR SIGN WITH** area. You are redirected to the login page of the selected service. Follow the instructions to link your account to Bitdefender Mobile Security.



Note

Bitdefender does not get access to any confidential information such as the password of the account you use to log in, or the personal information of your friends and contacts.

Activating Bitdefender Mobile Security

To be protected by Bitdefender Mobile Security, you must activate your product with a subscription, which specifies how long you may use the product. As soon as it expires, the app stops performing its functions and protecting your device.

To activate Bitdefender Mobile Security:

1. Open Bitdefender Mobile Security.
2. The app displays information regarding the current subscription status.

Tap **I HAVE A CODE**.

3. Type an activation code in the corresponding field, then tap **ACTIVATE**.

To extend an available subscription:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **My Account** from the list.
3. Under the **Extend subscription** section, type an activation code, and then tap **ACTIVATE**.

Alternatively you can extend your current subscription by accessing the listed offers.



Dashboard

Tap the Bitdefender Mobile Security icon in your device's app drawer to open the app interface.

The Dashboard offers information about the security status of your device and allows you to easily manage all security features.

Whenever there is a process in progress or a feature requires your input, a card with more information and possible actions is displayed in the Dashboard.

You can access the Bitdefender Mobile Security features and easily navigate from a section to another from the **Menu** button located in the upper-left corner of the screen:

Malware Scanner

Allows you to initiate an on-demand scan and enable or disable Scan Storage. For more information, refer to *"Malware Scanner"* (p. 7).

Account Privacy

Checks if any data leakage has occurred in your online accounts. For more information, refer to *"Account Privacy"* (p. 10).

Web Protection

Allows you to turn the web protection feature on or off. For more information, refer to *"Web Protection"* (p. 12).

VPN

Encrypts internet communication, helping you maintain your privacy no matter what network you are connected to. For more information, refer to *"VPN"* (p. 14).

Anti-Theft

Allows you to turn the Anti-Theft features on or off and to configure Anti-Theft settings. For more information, refer to *"Anti-Theft Features"* (p. 17).

App Lock

Allows you to protect your installed apps by setting a PIN access code. For more information, refer to *"App Lock"* (p. 22).

Reports

Keeps a log of all important actions, status changes and other critical messages related to your device's activity. For more information, refer to *"Reports"* (p. 27).



WearON

Communicates with your smartwatch to help you find your phone in case you misplace or forget where you left it. For more information, refer to *“WearON”* (p. 28).



3. MALWARE SCANNER

Bitdefender protects your device and data against malicious apps using on-install scanning and on-demand scanning.



Note

Make sure your mobile device is connected to the internet. If your device is not connected to the internet, the scan process will not start.

● On-install scanning

Whenever you install an app, Bitdefender Mobile Security automatically scans it using in-the-cloud technology. The same scanning process starts each time the installed apps are updated.

This type of scan is provided through the Autopilot feature. Autopilot is a smart scanner that scans all apps you install or update, and stops threats in their tracks.

If the app is found to be malicious, an alert will appear prompting you to uninstall it. Tap **Uninstall** to go to that app's uninstall screen.

● On-demand scanning

Whenever you want to make sure that the apps installed on your device are safe to use, you can initiate an on-demand scan.

To start an On-demand scan, simply tap the **START SCAN** button from the Malware Scanner card available in the Dashboard.

Alternatively, you can run a scan by following these steps:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **Malware Scanner** from the list.
3. Tap **START SCAN**.



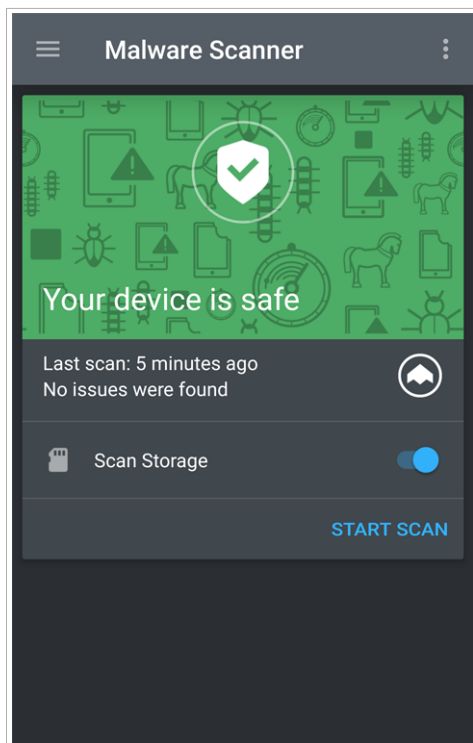
Note

Additional permissions are required on Android 6 for the Malware Scanner feature. After tapping the **START SCAN** button, select **Allow** for the following:

- Allow **Antivirus** to make and manage phone calls?
- Allow **Antivirus** to access photos, media, and files on your device?



The scan progress will be displayed and you can stop the process at any time.




Malware Scan

By default, Bitdefender Mobile Security will scan your device's internal storage, including any mounted SD card. This way, any dangerous apps that might be on the card can be detected before they can cause harm.

To enable or disable the Scan Storage setting:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **Malware Scanner** from the list.
3. Tap the corresponding switch.



You can also enable or disable the storage scanning from the **Settings** area by tapping the  button, then the corresponding switch.

If any malicious apps are detected, information about them will be displayed and you can remove them by tapping the **UNINSTALL** button.

The Malware Scanner card displays the state of your device. When your device is safe, the card is green. When the device requires a scan, or there is any action that requires your input, the card will turn red.



4. ACCOUNT PRIVACY

Bitdefender Account Privacy detects if any data leakage has occurred in the accounts you use for making online payments, shopping, or signing in different apps or websites. The data that may be stored into an account can be passwords, credit card information, or bank account information, and, if not properly secured, identity theft or invasion to privacy may occur.

The privacy status of an account is displayed right after validation.

Automatic rechecks are set to run in the background, but manual scans can be run as well on a daily basis.

Notifications will be displayed each time new leaks that include any of the validated email accounts are discovered.

To start keeping personal information safe:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **Account Privacy** from the list.
3. Tap the blue circle in the bottom right of the screen.
4. Type your email address in the corresponding field, and then tap **NEXT**.

Bitdefender needs to validate this account before displaying private information. Therefore, an email with a validation code is sent to the provided email address.

5. Check your inbox, and then type the received code in the **Account Privacy** area of your app. If you cannot find the validation email in the Inbox folder, check the Spam folder.


The privacy status of the validated account is displayed.

If leaks are found in any of your accounts, we recommend you to change their password as soon as possible. To create a strong and secure password, take into consideration these tips:

- Make it at least eight characters long.
- Include lower and upper case characters.
- Add at least one number or symbol, such as #, @, % or !.

Once you secured an account that was part of a privacy breach, you can confirm the changes by marking the identified leak(s) as **Solved**. To do this:



1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **Account Privacy** from the list.
3. Tap the account you just secured.
4. In the **Leaks** area, swipe left on the leak you secured the account for.
5. Tap the  icon.
6. The **Mark as solved** card appears.

Tap **CONFIRM** to acknowledge that the account is secured.

When all the detected leaks are marked as **Solved**, the account will no longer appear as leaked, at least until a new leakage is detected.



5. WEB PROTECTION

Web Protection checks using Bitdefender cloud services webpages you access with the default Android browser, Google Chrome, Firefox, Opera, Opera Mini and Dolphin. A complete list with the supported browsers is available in the Web Protection section.

If an URL points to a known phishing or fraudulent website, or to malicious content such as spyware or viruses, the webpage is temporarily blocked and an alert is shown.

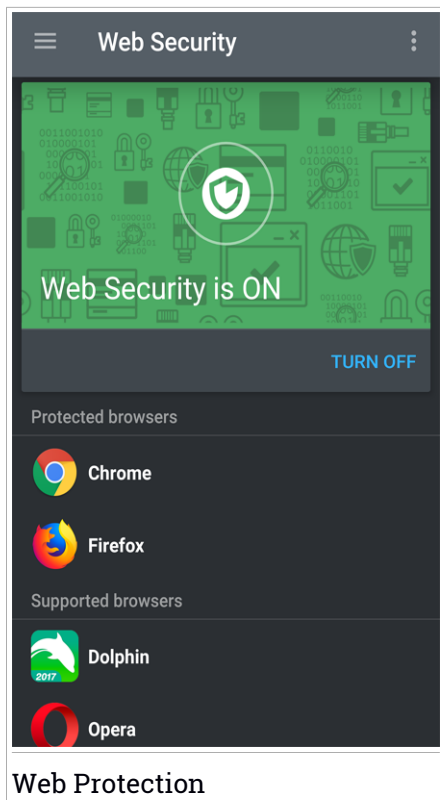
You can then choose to ignore the alert and proceed to the webpage or return to a safe page.



Note

Additional permissions are required on Android 6 for the Web Protection feature.

Allow permission to register as Accessibility service and tap **TURN ON** when requested. Tap **Antivirus** and enable the switch, then confirm that you agree with the access to your device's permission.





6. VPN

With Bitdefender VPN you can keep your data private each time you connect to unsecured wireless networks while in airports, malls, cafés, or hotels. This way, unfortunate situations such as theft of personal data, or attempts to make your device's IP address accessible to hackers can be avoided.

The VPN serves as a tunnel between your device and the network you connect to securing your connection, encrypting the data using bank-grade encryption, and hiding your IP address wherever you are. Your traffic is redirected through a separate server; thus making your device almost impossible to be identified through the myriad of the other devices that are using our services. Moreover, while connected to the internet via Bitdefender VPN, you are able to access content that is normally restricted in specific areas.



Note

Some countries practice internet censorship and therefore the usage of VPNs on their territory has been banned by law. To avoid legal consequences, a warning message can appear when you try to use the Bitdefender VPN feature for the first time. By continuing using the feature, you confirm that you are aware of the applicable country regulations and the risks to which you might be exposed.

There are two ways to turn on or off Bitdefender VPN:

- Tap the power on button in the VPN card from the Dashboard.

The status of Bitdefender VPN is displayed.

- Tap the **Menu** button and select **VPN** from the list.


Tap **CONNECT** each time you want to stay protected while connected to unsecured wireless networks.

Tap **DISCONNECT** whenever you want to disable the connection.



Note

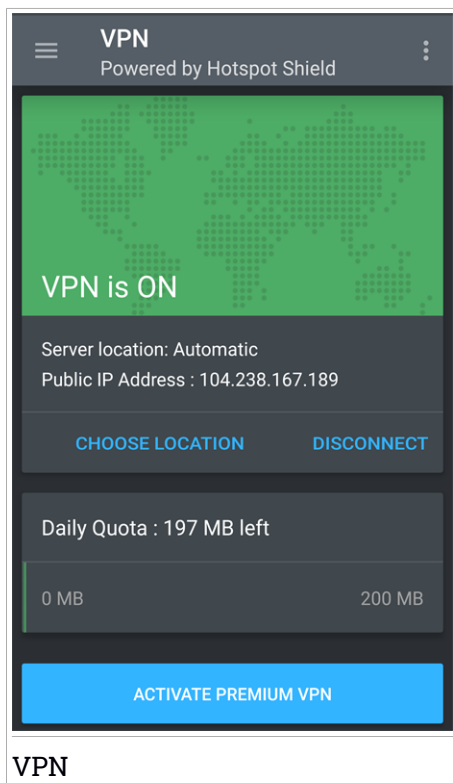
The first time you turn on VPN, you are asked to allow Bitdefender to set up a VPN connection that will monitor network traffic. Tap **OK** to continue.

The  icon appears in the status bar when Bitdefender VPN is active.

To save battery power, we recommend you to turn off the VPN feature when you do not need it.



If you have a premium subscription and would like to connect to a server at your will, tap **CHOOSE LOCATION** in the VPN feature, and then select the location you want. For details about VPN subscriptions, refer to **“Subscriptions” (p. 16)**.




Tap **MORE DETAILS** in the VPN card from the Dashboard to access the feature where you can:

- View how much traffic you have left from your daily quota or upgrade to the premium version - info available in the VPN free version.
- Choose the server you would like to connect to and view how much time is left from your subscription - info available in the Premium VPN version.



VPN Settings

Tap the  button in the VPN feature menu, then select **Settings** for an advanced configuration of your VPN.

In VPN **Settings** you can configure the following options:

- Quick access VPN notification - a notification will appear in the status bar to allow you to quickly turn on VPN.
- Notification when connecting to an open Wi-Fi - each time you connect to an open Wi-Fi network, you are notified in the status bar to use VPN.
- Notification when accessing a banking site - each time you access a banking site, you are notified in the status bar to use VPN.

Subscriptions

Bitdefender VPN offers for free a daily 200 MB traffic quota per device to secure your connection every time you need, and connects you automatically to the optimal server location.

To get unlimited traffic and unrestricted access to content worldwide by choosing a server location at your will, upgrade to the premium version.

You can upgrade to the Bitdefender Premium VPN version anytime by tapping the **ACTIVATE PREMIUM VPN** button available in the Dashboard or in the VPN window.

The Bitdefender Premium VPN subscription is independent from the Bitdefender Mobile Security subscription, meaning you will be able to use it for its entire availability, regardless of the state of your security subscription. In case the Bitdefender Premium VPN subscription expires, but the one for Bitdefender Mobile Security is still active, you will be reverted to the free plan.

Bitdefender VPN is a cross-platform product, available in the Bitdefender products compatible with Windows, macOS, Android, and iOS. Once you upgrade to the premium plan, you will be able to use your subscription on all products, provided that you login with the same Bitdefender account.



7. ANTI-THEFT FEATURES

Bitdefender can help you locate your device and prevent your personal data from getting into the wrong hands.

All you need to do is activate Anti-Theft from the device and, when needed, access **Bitdefender Central** from any web browser, anywhere.

Even if you cannot access the internet, you can still protect your device and data by sending **SMS commands** from any mobile phone to your smartphone through regular text messages.

Bitdefender Mobile Security offers the following Anti-Theft features:

Remote Location

View your device's current location on Google Maps. The location is refreshed every 5 seconds, so you can track it if it is on the move.

The accuracy of the location depends on how Bitdefender is able to determine it:

- If the GPS is enabled on the device, its location can be pinpointed to within a couple of meters as long it is in the range of GPS satellites (i.e. not inside a building).
- If the device is indoors, its location can be determined to within tens of meters if Wi-Fi is enabled and there are wireless networks available in its range.
- Otherwise, the location will be determined using only information from the mobile network, which can offer an accuracy no better than several hundred meters.

Show IP

Displays the last IP address for the selected device. Tap **SHOW IP** to make it visible.

Remote Wipe

Remove all personal data from your estranged device.

Remote Lock

Lock your device's screen and set a numeric PIN for unlocking it.

Send alert to device (Scream)

Remotely send a message to be displayed on the device's screen, or trigger a loud sound to be played on the device speaker.



If you lose your device, you can let whoever finds it know how they can return it to you by displaying a message on the screen of the device.

If you misplaced your device and there is a chance it is not far from you (for example, somewhere around the house or the office), what better way to find it than to make it play a loud sound? The sound will be played even if the device is in silent mode.

Activating Anti-Theft

To enable Anti-Theft features, simply complete the configuration process from the Anti-Theft card available in the Dashboard.

Alternatively, you can activate Anti-Theft by following these steps:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **Anti-Theft** from the list.
3. Tap **TURN ON**.
4. The following procedure will begin to help you activate this feature:



Note

Additional permissions are required on Android 6 for the Anti-Theft feature. To enable it, follow the steps below:

- Tap **Activate Anti-Theft**, then tap **TURN ON**.
- Allow permissions for the following:
 - a. Allow **Antivirus** to send and view SMS messages?
 - b. Allow **Antivirus** to access this device's location?
 - c. Allow **Antivirus** to access your contacts?

a. Grant Admin Privileges

These privileges are essential to the operation of the Anti-Theft module and therefore must be granted to continue.

b. Set Application PIN

To make sure any changes made to Anti-Theft settings are authorized by you, a PIN must be set. Every time an attempt will be made to modify Anti-Theft settings, the PIN will have to be entered before the changes are applied. Alternatively, on devices that support fingerprint



authentication, a fingerprint confirmation can be used instead of the configured PIN code.



Note

The same PIN code is used by App Lock to protect your installed apps.

c. Activate Snap Photo

Each time someone will try to access your installed apps while the Snap Photo option is turned on, Bitdefender will take a screenshot of him. For more details about this feature, refer to “**Snap Photo**” (p. 24).

d. Set Trusted Number for Anti-Theft

Select the **SMS CONTROL** tab, type a trusted phone number or select one from the contacts list, and then tap **SAVE NUMBER**. The trusted number should contain a country code and can be the number of someone you know, or the number of another phone you use.

When a different SIM card is inserted into your device, Bitdefender Mobile Security automatically sends a text message to the trusted number containing the new phone number.

This way, you can send SMS commands to your phone even if the SIM card is switched and its number changes.



Important

This is not a mandatory step, but it is recommended that you set the trusted number during the initial setup. The Wipe command works only when sent from the predefined trusted number.

Once Anti-Theft is activated, you can turn on or off Web control and SMS control features individually from the Anti-Theft screen by tapping the corresponding buttons.

Using Anti-Theft features from Bitdefender Central (Web Control)





Note

All Anti-Theft features require the **Background data** option to be enabled in your device's Data usage settings.



To access the Anti-Theft features from your Bitdefender account:

1. Access **Bitdefender Central**.
2. Tap the  icon in the upper-left corner of the screen, then select **My Devices**.
3. In the **MY DEVICES** window, select the desired device card.
4. Select the **Anti-Theft** tab.
5. In the bottom field of the window, tap the  icon, and then the button corresponding to the feature you want to use:

Locate - display your device's location on Google Maps.



Alert - type a message to display on your device's screen and/or make your device play a sound alarm.



Lock - lock your device and set a PIN code for unlocking it.



Wipe - delete all data from your device.



Important

After you wipe a device, all Anti-Theft features cease to function.

SHOW IP - displays the last IP address for the selected device.

Using Anti-Theft features through SMS commands (SMS Control)

Once SMS commands are enabled, you can send the following commands to your smartphone via SMS from any other mobile phone:

- **LOCATE** - send a message containing the location of the device to the phone number from which the command was sent. The message contains a Google Maps link which can be opened in the browser of the mobile phone.
- **SCREAM** - play a loud sound on the device speaker.
- **LOCK** - lock the device's screen with the PIN code you set.
- **WIPE** - delete all data from your device.



Important

The Wipe command works only when sent from the predefined trusted number.

- **CALLME** - dial the phone number from which the command was sent with the speaker turned on. This way you can silently listen on whoever has your phone.
- **HELP** - send a message containing all available commands to the phone number from which the command was sent.
- **SIM Change** - the trusted number you set will receive an SMS with the new phone number as soon as your SIM is replaced with a new one. To set up the phone number of your friend, tap the **Trusted number** option. Either type his number including the country code, or choose his card from the contacts list.

All SMS commands must be sent using the following format:

bd-<PIN> <command>



Note

The brackets indicate variables and should not appear in the command.

For example, if you have set the security PIN to 123456 and you want to receive a message with your phone's location, send the following text message to your phone number:

BD-123456 LOCATE



8. APP LOCK

Installed apps such as emails, photos, or messages, can contain personal data that you would like to remain private by selectively restricting access to them.

App Lock helps you block unwanted access to apps by setting a security PIN access code. The PIN code you set must be at least 4 digits long, but not more than 8, and is required every time you want to access the selected restricted apps.

Alternatively, on devices that support fingerprint authentication, a fingerprint confirmation can be used instead of the configured PIN code.

Activating App Lock

To restrict access to selected apps, configure App Lock from the card displayed in the Dashboard after activating Anti-Theft.

Alternatively, you can activate App Lock by following these steps:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **App Lock** from the list.
3. Tap **TURN ON**, and then allow access to usage data for Bitdefender by selecting the corresponding check box.



Note

Additional permissions are required on Android 6 for the Snap Photo feature. To enable it, allow **Antivirus** to take pictures and record video.

4. Go back to the app, configure the access code, and then tap **SET PIN**.



Note

This step is available only if you didn't previously configure the PIN in Anti-Theft.

5. Enable the Snap Photo option to catch any intruder that will try to access your private data.
6. Select the apps you want to protect.

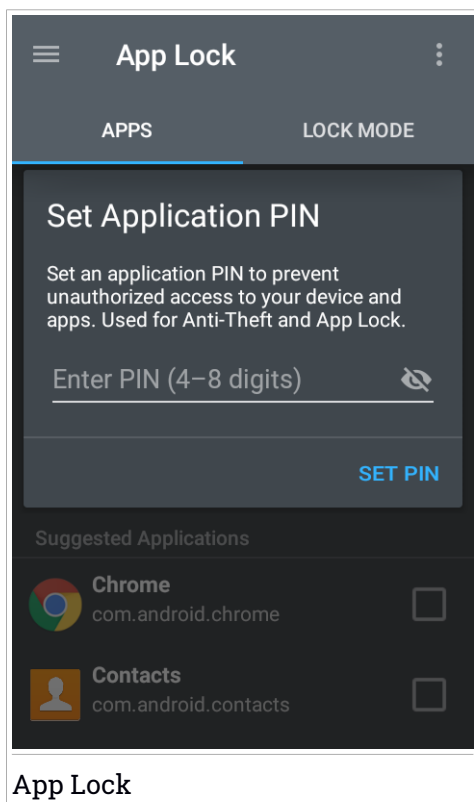


Using the wrong PIN or fingerprint five times in a row, will activate a 30 seconds time-out session. This way, any attempt to break in the protected apps will be blocked.



Note

The same PIN code is used by Anti-Theft to help you locate your device.



App Lock

Lock mode


From here you can choose when the App Lock feature should protect the apps installed on your device.

You can choose from one of the following options:



- **Lock every time** - the PIN code or fingerprint you have set up, will have to be used each time you access the locked apps.
- **Unlock until screen off** - the access to your apps will be valid until the screen turns off.
- **Allow a brief exit** - you can exit and access again your unlocked apps within 30 seconds.
- **Activate Smart Unlock** - when enabled and connected to a network set as trusted, the other settings are unavailable. This means no PIN or fingerprint confirmation is needed when accessing the locked apps.

App Lock Settings

Tap the  button in the App Lock feature menu, then select **Settings** for an advanced configuration of your App Lock.

In App Lock **Settings** you can do the following:

- Activate Snap Photo when three incorrect unlock attempts are made.
- Lock notifications for newly installed apps.
- Change your PIN code.

Snap Photo

With Bitdefender Snap Photo you can catch your friends or relatives on the hop. This way you can educate their curious eyes to not look through your personal files or the apps you use.

The feature works easy: each time the PIN code or fingerprint confirmation you set to protect your apps is entered wrong three times in a row, a photo is taken using the front camera. The photo is saved together with the time-stamp and reason, and can be seen when you open Bitdefender Mobile Security and access the App Lock feature.




Note

This feature is available only for phones that have a front camera.


To configure the Snap Photo feature:

1. Open Bitdefender Mobile Security.



2. Tap the **Menu** button, and select **App Lock** from the list.
 3. Tap the  button in the App Lock feature menu, and then select **Settings**.
 4. Enable the **Snap photo when 3 incorrect unlock attempts are made** switch.
- The photos snapped when the incorrect PIN is entered are displayed in the App Lock menu and can be viewed full-screen.

Alternatively, they can be viewed in your Bitdefender account:

1. Go to: <https://central.bitdefender.com>.
2. Sign in to your account.
3. Tap the  icon in the upper-left corner of the screen, then select **My Devices**.
4. Select your device from the **MY DEVICES** window, and then the **Anti-Theft** tab.

The photos are displayed.

Only the 3 most recent photos are saved.

Smart Unlock


An easy method to stop being asked by the App Lock feature to enter the PIN code or fingerprint confirmation for the protected apps each time you access them is to activate Smart Unlock.

With Smart Unlock you can set as trusted the Wi-Fi networks you usually connect to, and when connected to them, the App Lock blocking settings will be disabled for the protected apps.

To activate the Smart Unlock feature:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button, and select **App Lock** from the list.
3. Select the **LOCK MODE** tab, and then enable the corresponding switch.

The wireless network you are connected to is displayed.

To set the Wi-Fi connection you're currently using as trusted, tap the  icon.



Note

This setting is available only if the Smart Unlock feature is enabled.

Whenever you change your mind, disable the feature and the Wi-Fi networks you have set as trusted will be treated as untrusted.



9. REPORTS

The Reports feature keeps a detailed log of events concerning the scanning activity on your device.

Whenever something relevant to the security of your device happens, a new message is added to the Reports.

To access the Reports section:


1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **Reports** from the list.

The following tabs are available in the Reports window:

- **WEEKLY REPORTS** - here you have access to the security status and the performed tasks from the current and previous week. The current week's report is generated each Sunday and you will receive a notification informing you about it becoming available.

Each week a new tip will be displayed in this section, so make sure you check back regularly to get the best out of the app.

- **ACTIVITY LOG** - here you can check detailed information about the activity of your Bitdefender Mobile Security app since it was installed on your Android device.

To delete the available activity log, tap the  button in the upper-right corner of the screen, and then select **Clear Activity Log**.



10. WEARON

With Bitdefender WearON you can easily find your smartphone whether you left it at the office in a conference room or under a pillow on your couch. The device can be found even if the silent mode is activated.

Keep this feature enabled to make sure that you always have your smartphone at hand.



Note

The feature works with Android 4.3 and Android Wear.

Activating WearON

To use WearON, you only have to connect your smartwatch to the Bitdefender Mobile Security app and activate the feature with the following voice command:

Start:<Where is my phone>

Bitdefender WearON has two commands:

1. Phone Alert

With the Phone Alert feature you can quickly find your smartphone whenever you step too far away from it.

If you have your smartwatch with you, it automatically detects the app on your phone and vibrates whenever you are less than ten meters away from your device.

To enable this feature, open Bitdefender Mobile Security, tap **Global Settings** in the menu and select the corresponding switch under the WearON section.

2. Scream

Finding your phone has never been easier. Whenever you forget where you left your phone, tap the Scream command on your watch to make your phone scream.



11. SETTINGS

The Settings area is where you can make a set of changes to the following options:

- **Security PIN Code** - you can change the PIN code you set to unlock apps or Anti-theft commands.
- **Malware Scanner** - you can decide whether the storage should be scanned.
- **In-the-cloud detection** - you can decide whether to send us reports that may help us improve the cloud detection.
- **Account Privacy** - you can decide whether to stay informed when your accounts are not involved in leaks.
- **App Lock** - you can decide whether to lock notifications for newly installed apps.
- **Snap Photo** - you can decide whether a screenshot should be taken after three failed attempts to access your apps.
- **Anti-Theft** - you can change the number you set as trusted in case your device falls into foreign hands.
- **Reports** - you can decide whether to receive reports notifications.
- **Send anonymous reports** - you can decide whether to send us reports containing information about how you use the product. This information is essential for improving the product and can help us provide a better experience in the future.



12. ABOUT

To find information about the Bitdefender Mobile Security version you have installed, access the **About** area. In the same area you can contact us for support, access and read the Subscription Agreement and Privacy Policy, and view the Open-source licenses.



13. BITDEFENDER CENTRAL

Bitdefender Central is the web platform where you have access to the product's online features and services and can remotely perform important tasks on devices Bitdefender is installed on. You can log in to your Bitdefender account from any computer or mobile device connected to the internet by going to <https://central.bitdefender.com>. Once you have access to it, you can start doing the following:

- Download and install Bitdefender on Windows, macOS, iOS and Android operating systems. The products available for download are:
 - Bitdefender Mobile Security
 - Bitdefender Mobile Security for iOS
 - Bitdefender Antivirus for Mac
 - The Bitdefender Windows product line
- Manage and renew your Bitdefender subscriptions.
- Add new devices to your network and manage them wherever you are.

Accessing your Bitdefender account

To access your Bitdefender account, simply:

1. Open a web browser on any device with internet access.
2. Go to: <https://central.bitdefender.com>.
3. Log in to your account using your email address and password.



My Devices

The **MY DEVICES** area in your Bitdefender account gives you the possibility to install, manage and take remote actions on your Bitdefender product on any device, provided that it is turned on and connected to the internet. The device cards display the device name, protection status and if there are security risks affecting the protection of your devices.



To easily identify your devices, you can customize the device name:

1. Access [Bitdefender Central](#).



2. Tap the  icon in the upper-left corner of the screen, then select **My Devices**.
3. Tap the desired device card, and then the  icon in the upper-right corner of the screen.
4. Select **Settings**.
5. Type in a new name in the **Device name** field, then select **SAVE**.

You can create and assign an owner to each of your devices for better management:

1. Access **Bitdefender Central**.
2. Tap the  icon in the upper-left corner of the screen, then select **My Devices**.
3. Tap the desired device card, and then the  icon in the upper-right corner of the screen.
4. Select **Profile**.
5. Tap **Add owner**, and then fill in the corresponding fields. Customize the profile by adding a photo and selecting a date of birth.
6. Tap **ADD** to save the profile.
7. Select the desired owner from the **Device owner** list, then tap **ASSIGN**.

For more remote actions and information regarding your Bitdefender product on a specific device, select the desired device card.

Once you select a device card, the following tabs are available:

- **Dashboard**. In this window you can view details about the selected device, check its protection status, the status of Bitdefender VPN and how many threats have been blocked in the last seven days. The protection status can be green, when there is no issue affecting your device, yellow when the device needs your attention or red when the device is at risk. When there are issues affecting your device, tap the drop-down arrow in the upper status area to find out more details. From here you can manually fix issues that are affecting the security of your devices.
- **Protection**. From this window you can remotely run a Scan on your device. Tap the **SCAN** button to start the process. You can also check when the



last scan was performed on the device and a report of the latest scan with the most important information is available.


- **Anti-Theft.** In case you misplaced your device, with the Anti-Theft feature you can locate it and take remote actions. Tap **LOCATE** to find out the position of the device. The last known position will be displayed, along with the time and date. For more details about this feature, refer to *"Anti-Theft Features"* (p. 17).

My Subscriptions

The Bitdefender Central platform gives you the possibility to easily manage the subscriptions you have for all your devices.

Check available subscriptions

To check your available subscriptions:

1. Access **Bitdefender Central**.
2. Tap the  icon in the upper-left corner of the screen, then select **My Subscriptions**.

Here you have information about the availability of the subscriptions you own and the number of devices using each of them.

You can add a new device to a subscription or renew it by selecting a subscription card.

Add a new device

If your subscription covers more than one device, you can add a new device and install your Bitdefender Mobile Security on it, as described in *"Installing Bitdefender Mobile Security"* (p. 2).

Renew subscription

If there are less than 30 days from your subscription, and you opted out for automatically renewing, you can manually renew by following these steps:

1. Access **Bitdefender Central**.
2. Tap the  icon in the upper-left corner of the screen, then select **My Subscriptions**.



3. Select the desired subscription card.

4. Tap **RENEW** to continue.

A webpage opens in your web browser where you can renew your Bitdefender subscription.



14. FREQUENTLY ASKED QUESTIONS

Why does Bitdefender Mobile Security require an internet connection?

The app needs to communicate with Bitdefender servers to determine the security status of the apps it scans and of the webpages you are visiting, and also to receive commands from your Bitdefender account, when using the Anti-Theft features.



What does Bitdefender Mobile Security need each permission for?

- Internet access -> used for cloud communication.
- Read phone state and identity -> used to detect if the device is connected to the internet and to extract certain device info needed to create a unique ID when communicating to Bitdefender cloud.
- Read and write browser bookmarks -> Web Protection module deletes malicious sites from your browsing history.
- Read log data -> Bitdefender Mobile Security detects traces of threat activities from the Android logs.
- Read / write SMS, contacts, account data and external storage -> Required for the remote wipe feature.
- Location -> required for remote location.
- Camera -> required for Snap photo.
- Storage -> used to allow the Malware Scanner to check the SD card.

Where can I see details about the app's activity?

Bitdefender Mobile Security keeps a log of all important actions, status changes and other critical messages related to its activity. To access this information open Bitdefender Mobile Security and tap the **Menu** button, then select **Reports** from the list.

I forgot the PIN code that I set to protect my app. What do I do?

1. Access **Bitdefender Central**.
2. Tap the  icon in the upper-left corner of the screen, then select **My Devices**.
3. Tap the desired device card, and then the  icon in the upper-right corner of the screen.



4. Select **Settings**.
5. Retrieve the PIN code from the **Application PIN** field.

How will Bitdefender Mobile Security impact my device's performance and battery autonomy?



We keep the impact very low. The app only runs when it is essential - after you install an app, when you browse the app interface or when you want a security check. Bitdefender Mobile Security does not run in the background when you call your buddies, type a message or play a game.

How can I switch off the App Lock feature?

There is no turn off option for the App Lock feature, but you can easily disable it by clearing the check boxes next to the selected apps after validating the PIN or fingerprint you have set.


How can I set another wireless network as trusted?

If you want to set another wireless network as trusted:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **App Lock** from the list.
3. Select the **LOCK MODE** tab, and then select the  icon.
4. Validate the PIN or fingerprint to confirm your choice.
5. Tap the  icon next to the network you want to set as trusted.

How can I stop seeing snapped photos taken on my devices?

To stop making visible the snapped photos taken on your devices:

1. Access **Bitdefender Central**.
2. Tap the  icon in the upper right side of the screen.
3. Tap **My Account** in the slide menu.
4. Select the **Settings** tab.
5. Disable the **Show/don't show snap photos taken on your devices** option.

How can I keep my online shopping secure?

Online shopping comes with high risks when some details are ignored. To not become a victim of fraud, we recommend you the following:

- Keep your security app updated.



- Submit online payments only with buyer protection.
- Use a VPN when connecting to the internet from public and unsecured wireless networks.
- Pay attention to the passwords you have assigned to your online accounts. They have to be strong including capital and lowercase letters, numbers and symbols (@, !, %, #, etc.).
- Make sure that the information you send is over secure connections. The online website extension has to be HTTPS://, and not HTTP://.

When should I use Bitdefender VPN?

You have to be careful when you access, download, or upload content on the internet. To make sure you stay safe while browsing the web, we recommend you to use Bitdefender VPN when you:

- want to connect to public wireless networks
- want to access content that normally is restricted in specific areas, no matter you are home or abroad
- want keep your personal data private (usernames, passwords, credit card information, etc.)
- want to hide your IP address

Will Bitdefender VPN have a negative impact on the battery life of my device?

Bitdefender VPN is designed to protect your personal data, hide your IP address while connected to unsecured wireless networks, and access restricted content in certain countries. To avoid an unnecessary battery consumption of your device, we recommend you to use the VPN only when you need it, and disconnect when offline.

Why am I encountering internet slowdowns while connected with Bitdefender VPN?

Bitdefender VPN is designed to offer you a light experience while surfing the web; however, your internet connectivity or the server distance you connect to may cause the slowdown. In this case, if it is not a must to connect from your location to a faraway hosted server (e.g. from USA to China), we recommend you to allow Bitdefender VPN to automatically connect you to the nearest server, or find a server closer to your current location.

Can I change the Bitdefender account linked to my device?



Yes, you can easily change the Bitdefender account linked to your device by following these steps:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **My Account** from the list.
3. Tap **LOGOUT**, and then confirm your choice.
4. Tap **USE CENTRAL ACCOUNT**, and then type your new Bitdefender account email address and password.

What is Device Administrator?

Device Administrator is an Android feature that gives Bitdefender Mobile Security the permissions needed to perform certain tasks remotely. Without these privileges, remote lock would not work and device wipe would not be able to completely remove your data. If you want to remove the app, make sure to revoke these privileges before trying to uninstall from **Settings > Security > Select device administrators**.

What's the trusted number for?

If your phone gets into the hands of someone who has no intention of returning it to its rightful owner, it is likely that the SIM card will be changed quickly. Whenever Bitdefender Mobile Security detects the SIM card in your phone has been changed, it automatically sends a text message containing the new phone number to the number you have set. This way, you can send SMS commands to your phone even if the SIM card is switched and its number changes. This can be the phone number of someone you know and trust, or the number of another phone you use.

Can the trusted number be changed after I set it?

To set a different trusted number:

1. Open Bitdefender Mobile Security.
2. Tap the **Menu** button and select **Settings** from the list.
3. Under the **Anti-Theft** section, tap **Trusted number**.

You will be prompted to provide the PIN before you can change the trusted number.

How much will it cost me to send SMS commands?

SMS commands are sent as regular text messages and are therefore charged as such by your carrier. Bitdefender does not charge any extra fees.



How to fix "No Google Token" error that appears when signing in to Bitdefender Mobile Security.

This error occurs when the device is not associated with a Google account, or the device is associated with an account but a temporary problem is preventing it from connecting to Google. Try one of the following solutions:

- Go to Android Settings > Applications > Manage Applications > Bitdefender Mobile Security and tap **Clear data**. Then try to sign in again.

- Make sure your device is associated with a Google account.

To check this, go to Settings > Accounts & sync and see if a Google account is listed under **Manage Accounts**. Add your account if one is not listed, restart your device and then try to sign in to Bitdefender Mobile Security.

- Restart your device, and then try to sign in again.

In what languages is Bitdefender Mobile Security available?

Bitdefender Mobile Security is currently available in the following languages:

- Brazilian
- Czech
- Dutch
- English
- French
- German
- Greek
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Romanian
- Russian
- Spanish
- Thai
- Turkish
- Vietnamese



Other languages will be added in future releases. To change the language of the Bitdefender Mobile Security interface, go to your device's **Language & keyboard** settings and set the device to the language you want to use.



15. GETTING HELP

Several online resources are available to help you solve your Bitdefender-related problems and questions.

- Bitdefender Support Center:

<https://www.bitdefender.com/support/consumer.html>

- Bitdefender Support Forum: <https://forum.bitdefender.com>

- The HOTforSecurity computer security portal:

<https://www.hotforsecurity.com/>

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

Bitdefender Support Center

The Bitdefender Support Center is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bug fixing activities of the Bitdefender support and development teams, along with more general articles about threat prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Support Center is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Support Center, as bugfix reports, workaround cheatsheets or informational articles to supplement product help files.

The Bitdefender Support Center is available any time at <https://www.bitdefender.com/support/>.

Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others.



If your Bitdefender product does not operate well, if it cannot remove specific threats from your device or if you have questions about the way it works, post your problem or question on the forum.

Bitdefender support technicians monitor the forum for new posts to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, search the forum for a similar or related topic.

The Bitdefender Support Forum is available at <https://forum.bitdefender.com>, in 5 different languages: English, German, French, Spanish and Romanian. Tap the **Home & Home Office Protection** link to access the section dedicated to consumer products.

HOTforSecurity Portal

The HOTforSecurity portal is a rich source of security information. Here you can learn about the various threats your computer is exposed to when connected to the internet (malware, phishing, spam, cyber-criminals). A useful dictionary helps you understand the computer security terms that you are not familiar with.

New articles are posted regularly to keep you up-to-date with the latest threats discovered, the current security trends and other information on the computer security industry.

The HOTforSecurity webpage is <https://hotforsecurity.bitdefender.com/>.